REMARKS

Applicant respectfully requests reconsideration of the present application in view of the amendments set forth above and the below remarks.

Claims 1-28 and 38-45 are pending in the application; claims 29-37 were previously canceled without prejudice due to a previous restriction requirement.

Claim Rejections Under §101

Claims 1, 2, 4-17, 19-28, and 40-45 are rejected under 35 U.S.C. §101. Applicant makes claim amendments to include an outputting element. Applicant does not necessarily agree with the Examiner's rejections and makes these amendments to expedite allowance of the case and not for reasons of patentability.

The Prior Art Rejections

Claims 1-3, 6-9, 11, 12, 14-17, 19-23, 26-28 and 38-44 are rejected under 35 U.S.C. §102(b) over Alabbadi et al., "Integrated Security and Error Control for Communication Networks Using the McEliece Cryptosystem."

Applicant submits that the Examiner has given no patentable weight to, the claim term "an order-invariant fuzzy commitment." As discussed throughout the specification, the order of the elements in the sequence used to form the fuzzy commitment does not matter. For example, at pages 5-6 of Applicant's specification and exemplary embodiment of the claimed invention is described as set forth below (emphasis added):

> FIGs. 1-2 show an exemplary system 100 having an order-invariant fuzzy commitment scheme in accordance with the present invention. The system 100 enables a user to commit (or encrypt) an item of information, such as a plaintext κ, under a first set or list E of distinct elements in universe U. The resultant cipher can be decommitted under a second list D that overlaps to a predetermined level with the first list E. *The ordering of the first and second lists E, D has essentially*

no influence on the commitment or decommitment process. The system is also *tolerant of bit-level errors*.

In an exemplary embodiment, Alice desires to commit a plaintext κ under a first list E. In one embodiment, a polynomial p in a single variable is selected such that the polynomial p encodes plaintext κ. Alice computes evaluations of p on input values corresponding to the elements of the first list E. More particularly, Alice projects a set of values specified by the first list E onto points that lie on the polynomial p. Alice then selects a number of random "chaff" points that do not lie on the polynomial p.

It is understood that chaff refers to the intentional addition/corruption of data to thwart an attacker. The entire collection of points, both those that lie on the polynomial p and the random chaff points, together constitute a commitment of p (that is, κ), which can be referred to a collection of points or target set R.

As shown in FIG. 3, the first list E can be considered to identify points in R that lie on the polynomial p, so as to specify the polynomial p. The elements in the list E can be mapped to the x-axis and corresponding points on the y-axis, such that $y_i=p(x_i)$. Other points are chaff points C for thwarting an attacker from discovering any information encoded under the list E. The collection of points R includes the points in E, which lie on the polynomial p, and the chaff points C, which do not lie on the polynomial to confuse an attacker.

Bob can attempt to decommit the plaintext κ with a second list D. If the second list D overlaps "substantially" with the first list E, as defined below, then *the second list D identifies points in R that lie on the polynomial p* to enable Bob to recover a set of points that is largely correct. *Using error correction, which can be in the form of an error-correcting code, Bob is then able to reconstruct the polynomial p, and thereby the plaintext* κ. If the second list D does not overlap substantially with the first list E, then it is infeasible for Bob to learn κ. If D overlaps "somewhat", then he may still be able to recover κ, as described below.

Applicant believes that the Examiner has confused error correction used in exemplary embodiments of the claimed order-invariant fuzzy commitment and error correction in Alabbadi. The Alabbadi scheme assumes that the party performing the decoding step holds a private key that may be *unknown to the encoding party*. In contrast, the proposed invention requires that the encoding party and decoding party *substantially share* knowledge of the encoding *secret*.

Further, revisiting the example from the Response to the first Office Action, if the original message is (A, B, C, D, E,) and the received message is (E, A, D, C, B), i.e., the ordering is different for each element, the error correcting code of Alabbadi will not be able to decode the received message. However, where the commitment is order invariant, the order of the elements does not matter in the invention as claimed. In addition, inserting errors into a *ciphertext* as taught by Alabbadi is completely different than *order invariance* as claimed.

Alabbadi does not teach commitment of a message and is not relevant to order invariance as claimed by Applicant. Alabaddi discloses a *public-key cryptosystem* for a data communication system. The underlying Goppa code in the McEliece public-key cryptosystem acts as *an error control system*, such as forward error correction (FEC). Errors are intentionally introduced to the *ciphertext* to increase decoding difficulty for unauthorized parties. In contrast to the present invention, in Alabbadi decryption does not recover any underlying polynomial since the decryptor knows the underlying polynomials in the cryptosystem from the private key.

In contrast, claim 1 requires a computer-implemented method for creating an *order-invariant fuzzy commitment*, comprising:

(a) receiving a first input element comprising a sequence of at least one value (a_1,..., a_n) from *a predetermined set*;

(b) generating a codeword of an error-correcting code for *generating the commitment*;

(c) constructing a first sequence of coordinate sets (x_i,y_i), for i in {1,...n}, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element and a second value (y_i) corresponding to a symbol in the codeword, wherein the symbol corresponds to the x_ith symbol in the codeword, wherein an *order-invariant fuzzy commitment* is formed.

The claimed invention is directed to a *commitment scheme* as understood by those of ordinary skill in the art. A *commitment scheme* permits one party to encrypt a message "m" under a key "k" as "C". A second party with knowledge of key k, or some close k' in accordance with the invention, can learn the message m and confirm that C was computed using the message m.

In contrast, Alabbadi teaches that a message m is encrypted under a public key PK; a second party needs a *private* key SK in order to recover the message m, where SK differs from PK. This is in contrast the invention as claimed which requires creating an order-invariant commitment of a predetermined set of values.

Further, Alabaddi does not even remotely teach decommitment made selectively on the basis of overlap between the transmitted message c and received message c'. The receiver does not know *a priori* what the degree of overlap is, and therefore cannot perform the operation selectively. Instead, the receiver in Alabbadi always executes the decryption operation, which succeeds only if the transmitted message c and received message c' are sufficiently similar, i.e., meet an *error* threshold.

For at least the above reasons, Applicant respectfully submits that claim 1 is patentably distinguishable over Alabbadi. For at least the same reasons, Applicant submits that claims 2-28 and 38-45 are also distinguishable over the cited references.

Applicant submits that certain dependent claims are further patentably distinguishable over the cited references. For example, claim 6 requires adding chaff to the first sequence. In the McEliece scheme and Alabbadi schemes, a message is converted into a *codeword* and then *perturbed*, i.e., errors are introduced. This is completely different than adding chaff to the *first sequence* as claimed.

Claim 10 is rejected under §103 over Alabbadi. For at least the reasons discussed above, Applicant submits that claim 10 is distinguishable over Alabaddi.

Claims 13 and 24 are rejected under §103 over Alabbadi in view of Rao.

Applicant submits that Rao does not overcome any of the deficiencies of Alabbadi discussed above. Rao merely discloses a private-key cryptosystem that uses simple codes of

distance and lengths of 250 bits or less for efficient encoding/decoding. Neither Alabaddi nor Rao, alone or in combination, disclose the invention as claimed.

In light of the above, Applicant submits that claims 1-28 and 38-45 are patentably distinguishable over the cited art. A notice of allowance for these claims is respectfully requested.

Applicant requests a telephone interview with the Examiner absent a Notice of Allowance filed in response to the accompanying RCE of which this response forms a part.

The Examiner is respectfully invited to telephone the undersigning attorney to discuss any matter in furtherance of the present application.

Applicant does not acquiesce to any assertion made by the Examiner not specifically addressed herein.

The Assistant Commissioner is hereby authorized to charge payment of any additional fees associated with this communication or credit any overpayment to Deposit Account No. 500845.

Respectfully submitted,

Dated: July 14, 2006

DALY, CROWLEY, MOFFORD & DURKEE, LLP

By: /Paul D. Durkee/

Paul D. Durkee
Reg. No. 41,003
Attorney for Applicant(s)
354A Turnpike Street - Suite 301A
Canton, MA 02021-2714
Tel.: (781) 401-9988, Ext. 21
Fax: (781) 401-9966
pdd@dc-m.com

25930